UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,526	08/16/2001	Arindam Das-Purkayastha	B-4274 618998-3	3735

22879 7590 05/15/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/931,526
Filing Date: August 16, 2001
Appellant(s): DAS-PURKAYASTHA ET AL.

Robert Popa
(Reg. No. 43,010)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8 January 2007 appealing from the Office action mailed 15 August 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Grawrock U.S Patent No. 6,678,833

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1 – 9, 11 – 19, 24 – 26, 28 – 37, 40, 42 – 55 and 58 are rejected under 35 U.S.C. 102(e) as being anticipated by Grawrock (U.S. Patent 6,678,833).

As per claim 1 and 6, Grawrock teaches a computer apparatus, comprising:

a receiver for receiving an integrity metric for a computer entity via a trusted device (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger) **associated with the computer entity, the integrity metric having values for a plurality of characteristics associated with the computer entity** (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15).

a controller for assigning a trust level to the computer entity from a plurality of trust levels, wherein the assigned trust level is based upon the value

of at least one of the characteristics of the received integrity metric (Grawrock: Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6: TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level). Please also see the detail rational of rejections set forth on Section (10) Response to Argument (Issue 1) of this Examiner Answer for expanded Examiner arguments.

As per claim 7, Grawrock teaches a method for establishing communications with a computer entity, comprising:

requesting a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device and containing values indicative of one or more characteristics of the entity; receiving a response from the trusted device including an integrity metric calculated for the entity by the trusted device (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger);

comparing values in the integrity metric (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer

entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15) **calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party** (Grawrock: Column 4 Line 9 and Column 4 Line 35 – 37: the challenger that verifies and determines the trust level (i.e. trusted or un-trusted) is interpreted as the trusted party that must provide the authentication values for comparing against the integrity metrics reported by the TPM so that whether the platform is trusted or not can be determined accordingly, as taught by Grawrock); and

selecting a level of trust for the entity from a plurality of predefined levels of trusts based on at least one value in the integrity metric calculated for the entity by the trusted device (Grawrock: Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6: TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level). Please also see the detail rational of rejections set forth on Section (10) Response to Argument (Issue 1) of this Examiner Answer for expanded Examiner arguments.

As per claim 24, Grawrock teaches a method for a computer entity to respond to a request for integrity check prior to exchanging data, comprising:

receiving at a trusted device associated with a computer entity a request to provide an integrity metric containing values indicative of one or more characteristics of the entity (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger);

calculating at the trusted device values indicative of one or more characteristics of the entity (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15); and providing a response from the trusted device including an integrity metric including the values indicative of one or more characteristics of the entity (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6). Please also see the detail rational of rejections set forth on Section (10) Response to Argument (Issue 1) of this Examiner Answer for expanded Examiner arguments.

As per claim 42, Grawrock teaches a method for establishing communications between a computer entity and a user, comprising:

presenting a request from the user to a trusted device associated with a computer entity to provide an integrity metric calculated for the entity by the trusted device; presenting to the user a response from the trusted device including an integrity metric calculated for the entity by the trusted device (Grawrock: Figure 3 / Element 230 and Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: the challenger is considered as the user, and TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger) and containing values indicative of one or more characteristics of the entity (Grawrock: Column 3 Line 56 – 61 and Column 4 Line 3 – 6: examples of the integrity metric associated with the computer entity, as taught by Grawrock, include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system – these integrity metrics also appear in the disclosure of the instant application (SPEC: Page 11 Line 10 – 15);

comparing at the user (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6: TPM module is considered as a trusted device that can accurately report the integrity metric upon the request issued by the challenger so that the challenger can determine that the platform has been properly initialized and is trusted) values in the integrity metric calculated for the entity by the trusted device with authenticated values provided for the entity by a trusted party (Grawrock: Column 4 Line 9 and Column 4 Line 35 – 37: the challenger that verifies and determines the trust level (i.e. trusted or un-trusted) is interpreted as the trusted party that must provide the authentication values for comparing against the integrity metrics reported by the TPM so

that whether the platform is trusted or not can be determined accordingly, as taught by Grawrock); and

selecting at the user a level of trust for the entity from a plurality of predefined levels of trusts available to the user based on at least one value in the integrity metric calculated for the entity by the trusted device (Grawrock: Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6: TPM module reports the integrity metric upon the request issued by the challenger so that the challenger can verify and determine that the platform has been properly initialized and is trusted upon the verification – i.e. to maintain a trust level or otherwise, an un-trusted level. Therefore, a broadest and reasonable interpretation is made to consider that a plurality of trust levels merely constitute a trusted level and an un-trusted level). Please also see the detail rational of rejections set forth on Section (10) Response to Argument (Issue 1) of this Examiner Answer for expanded Examiner arguments.

As per claim 2, Grawrock teaches the trusted device is arranged to acquire an integrity metric of the computer entity (Grawrock: Column 3 Line 62 – Column 4 Line 9).

As per claim 3, Grawrock teaches the trust level is determined by comparing the value of the at least one characteristics with a specified value (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6).

As per claim 4, Grawrock teaches the plurality of trust levels are determined base upon a plurality of specified values associated with a plurality of characteristics of a computer entity (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37 and Column 2 Line 5 – 6).

As per claim 5, Grawrock teaches the plurality of trust levels are determined based upon a plurality of specified values associated with characteristics for a plurality of computer entities (Grawrock: Column 4 Line 9 – 12, Column 4 Line 35 – 37, Column 4 Line 8 – 9 and Column 2 Line 5 – 6).

As per claim 8, 11, 25, 28, 43 and 46, Grawrock teaches the trusted device is hardwired to the computer entity (Grawrock: Column 4 Line 21 – 23).

As per claim 9, 26 and 44, Grawrock teaches the trusted device is configured to control the boot process of the computer entity (Grawrock: Column 3 Line 61 – 67).

As per claim 12, 29 and 47, Grawrock teaches the trusted device is configured to contain one or more of a public encryption key, a private encryption key (Grawrock: Column 4 Line 13 – 19: the TPM must contain the public / private key-pair; otherwise, the requested / response information can not be decrypted / encrypted properly), and one or more authenticated values provided for the entity integrity metric by the trusted party (Grawrock: Column 4 Line 9 and Column 4 Line 10 – 11: (a) the challenger

verifies the results and determines the trust level and as such the challenger must contain the respective authenticated values (b) the challenger can be an internal device within the TPM, as taught by Grawrock, and therefore authenticated values must be also within the TPM (i.e. challenger)).

As per claim 13, 30 and 48, Grawrock teaches the trusted device is configured to calculate the integrity metric by generating a digest of BIOS instructions in the BIOS memory of the entity (Grawrock: Column 3 Line 61 – 67 and Column 4 Line 7 – 9).

As per claim 14, 31 and 49, Grawrock teaches the trusted device is configured to calculate the integrity metric by measuring one or more values of configuration information regarding one or more components of the entity (Grawrock: Column 4 Line 1 – 9: the boot block identifiers can be considered as part of the system configuration information to trace different version# of BIOS code).

As per claim 15, 32, 36, 50 and 54, Grawrock teaches the components of the entity are selected from among the group of components comprising hardware components and software components (Grawrock: Column 4 Line 1 – 6).

As per claim 16, 33 and 51, Grawrock teaches wherein the components of the entity are selected from among the group of components comprising the BIOS, ROM,

operating system loader, and operating system of the entity (Grawrock: Column 4 Line 3 – 6).

As per claim 17, 34 and 52, Grawrock teaches the configuration information measured for at least one of the components comprises one or more of certificate information, last update information, latest update version information, and previous update information (Grawrock: Column 4 Line 15 – 18: for example, certificate).

As per claim 18, 35 and 53, Grawrock teaches the trusted device is configured to calculate the integrity metric by engaging in predetermined interactions with one or more components of the entity and acquiring the values of the responses of the one or more components (Grawrock: Column 4 Line 1 – 9).

As per claim 19, 37 and 55, Grawrock teaches the response received from the trusted device includes the authenticated values provided by the trusted party (Grawrock: Column 4 Line 35 – 40).

As per claim 40 and 58, Grawrock teaches the request includes input data (Grawrock: Column 4 Line 13 – 16).

2. Claims 10, 27 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (U.S. Patent 6,678,833), in view of Saunders (U.S. Patent 6,209,099).

As per claim 10, 27 and 45, Grawrock does not disclose expressly the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device.

Saunders teaches the trusted device is configured to not respond to the request for the integrity metric if the boot process of the computer entity was not controlled by the trusted device (Saunders: Figure 3 Element 28: no further response from the trusted device if the boot key is not entered and configured).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Saunders within the system of Grawrock because (a) Grawrock teaches protecting information and accurately reporting this information by using a trustworthy TPM (Trusted Platform Module) (Grawrock : Column 1 Line 65 – 67) and (b) Saunders teaches providing a mechanism to decide whether the components of the system (including both hardware and software components) are really trustworthy without modification (Saunders: Column 1 Line 11 – 17).

3. Claims 20, 21, 38, 39, 41, 56, 57 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (U.S. Patent 6,678,833), and in view of Stoltz (U.S. Patent 6,615,264).

As per claim 20, 38 and 56, Grawrock does not disclose expressly generating a nonce to pass to the trusted device with the request.

Stoltz teaches generating a nonce to pass to the trusted device with the request (Stoltz: Column 17 Line 64 – 66, Column 18 Line 1 – 5: nonce is a random number).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Stoltz within the system of Grawrock because (a) Grawrock teaches protecting information and accurately reporting this information by using a trustworthy TPM (Trusted Platform Module) with the request initiated from an external device (Grawrock : Column 1 Line 65 – 67 and Column 4 Line 12) and (b) Stoltz teaches a security enhanced method to authenticate the request for secure information in a client-server networking system – i.e. from an external device respective to the TPM system (Stoltz: Column 3 Line 65 – Column 4 Line 2, Column 4 Line 9 – 12, Column 17 Line 64 – 66 and Column 18 Line 1 – 5).

As per claim 21, 39 and 57, Grawrock as modified further teaches the response from the trusted device includes the nonce received with the request (Stoltz: Column 18 Line 46 – 47).

As per claim 41 and 59, Grawrock as modified teaches the response includes the input data processed with the private encryption key (Stoltz: Column 18 Line 41 – 43: the response includes the encryption of the random number, which is part of the input information during the request). See the same rationale address above in rejection claim 20.

4. Claims 22 – 23 and 60 – 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grawrock (U.S. Patent 6,678,833).

As per claim 22 and 60, Grawrock teaches the requester (or challenger – an external device) verifies and determines the trust level (i.e. trusted or un-trusted) of the respective computer entity with which it attempts for establishing communications Grawrock: Column 4 Line 9, Column 4 Line 35 – 37 and Column 4 Line 12: challenger is an external device). Grawrock does not disclose expressly initiating data transfer to the entity in accordance with the selected trust level.

Howeve, It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify Grawrock to accommodate initiating data transfer to the entity in accordance with the selected trust level because a person of ordinary skill would recognize the risk and avoid transferring data with an unsecured system once the trusted level (i.e. either trusted or un-trusted) of the target computer entity has been evaluated by the user / challenger / external device, as taught by Grawrock (Grawrock: Column 4 Line 35 – 37).

As per claim 23 and 61, Grawrock as modified further teaches initiating data transfer to the entity in accordance with the selected trust level comprises transferring no data (See the same rationale as set forth in rejecting claim 22).

(10) Response to Argument

In the instant appeal brief, Appellant has the presented the following arguments:

Issue 1. Claims 1 – 9, 11 – 19, 24 – 26, 28 – 37 40, 42 – 55 and 58:

Whether claims 1-9, 11-19, 24-26, 28-37, 40, 42-55 and 58 are patentable under 35 U.S.C. 102(e) over U.S. Pat. No. 6,678,833 to Grawrock (hereinafter "Grawrock").

(a) As per claim 1, Appellants submit that the Examiner's assertion that "software modules provided in a trusted platform module anticipate an integrity metric having values for a plurality of characteristics associated with a computer entity simply makes no sense (Brief: Page 6 / 3rd Para)".

- ✓ Examiner respectfully disagrees because Grawrock teaches "Similarly, during initialization, various software modules are provided to the TPM 230. Examples of the modules include BIOS 340, Option ROMs such as BIOS extensions 350, or even a OS loader 360 which is a portion of the operating system that is loaded into the system memory 130 to control loading of the operating system. As an option, these modules 340, 350 and 360 can undergo a hash operation to produce corresponding identifiers 345, 355 and 365 for later use in verification by a challenger (Grawrock: Column 4 Line 1 – 9 and Figure 3 / Element 340 & 345, 350 & 355 and 360 & 365)".

- ✓ Examiner notes each of hash identifiers (e.g. checksum) generated from each of software modules such as BIOS 340, Option ROMs, BIOS extensions 350, or even a OS loader 360 at a trusted device (Figure 3 / Element 230: i.e. TPM (Trusted Platform Module)), is used for authentication purpose in verification by a challenger to assure the integrity of a computer entity. Therefore, it is qualified as an integrity metric having values for a plurality of characteristics associated with a computer entity.
- ✓ This is also consistent with the disclosure of the specification of the instant application (SPEC: Page 11 Line 10 – 15), as shown below.

> Any computing apparatus should have a minimum number of CCRs (Component Configuration register) to hold information about the critical components. There is, as has been stated earlier, no upper limit of CCRs in a computing apparatus.
>
> Preferably a CCR is available for each of the following components:
> 1. BIOS
> 2. Optional ROM
> 3. OS Loader
> 4. Operating System

(b) As per claim 1, Appellants submit that Grawrock does not teach "assigning a trust level to the computer entity from a plurality of trust levels" because there is only one trust level disclosed in Grawrock – that is trusted (Brief: Page 7 Line 14 – 17)".

- ✓ Examiner notes the "un-trusted" and "trusted" levels (Grawrock: Column 4 Line 36 – 38 and Column 4 Line 6 – 9) are sufficient to constitute a plurality of trust

levels to meet the claim language and a plurality of trust levels must include the un-trusted level; otherwise, the system does not work, according to the disclosure of the specification. This is because the assigned trust level is based upon the value of at least one of the characteristics of the received integrity metric and therefore one of the measurement results must include the situation where each of the received characteristics of the integrity metric is consistently (i.e. non-exceptionally) negative and that renders the computer system being un-trustable to the users and as such the assigned trust level must be an un-trusted level. Therefore, based on the determination of trust level and un-trusted level from the authentication hash values such as BIOS, Optional ROM, OS Loader and etc., as taught by Grawrock, the determined trust level and un-trusted level is qualified and sufficient to constitute a plurality of trust levels, according to MPEP 2111, the broadest and reasonable claim interpretations are made by the Examiner. Besides, Examiner notes Appellants also admit there is a second trust level, which is an un-trusted level, as taught by the system of Grawrock (Brief: Page 7, 1st Para, Last sentence).

✓ In addition, Appellants argue that "various application programs can access various types of data depending on the trust level assigned to the computer entity in response to each user's challenge (Brief: Page 7)". Examiner notes Applicant's argument has no merit since the alleged limitation has not been recited into the claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See

In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Examiner notes the claim only requires a plurality of trust levels and the determined trust level and un-trusted level by Grawrock is sufficient to meet the claim language of a plurality of trust levels as set forth above.

(c) As per claim 1, Appellants argue that "determining that a platform is trusted is not the same as assigning a trust level (Brief: Page 7 Line 12 – 13)".

✓ Examiner respectfully disagrees because, in a computer system, the process of undergoing a hash calculation operation to produce a hash identifier for verification purpose (Grawrock: Column 4 Line 6 – 9) and to determine whether a computer entity is trusted or not (Grawrock: Column 4 Line 36 – 38) is not carried out merely in human mind and as such determining whether a platform is trusted or not is indeed assigning a trust level of a computer entity, either trusted or un-trusted, as admitted by Appellants indicating "Grawrock, which is merely informs a user whether the platform is trusted or not (Brief: Page 7 / Last line of 1st Para).

(d) As per claim 7, Appellants argue "there is no support in Grawrock that such a challenger is a trusted party that it has the authentication values for comparing against the integrity metrics allegedly reported by the TPM (Brief: Page 8 / 3rd Para)".

✓ Examiner notes, as set forth in the Final Office action submitted on 15 August 2006, a challenger that verifies and determines the trust level (i.e. trusted or un-

trusted) based on the hash identifiers (i.e. integrity metric) reported from the trusted device (TPM) can be interpreted as a trusted party that must have the authentication values for comparing against the reported / calculated integrity metrics (Grawrock: Column 4 Line 6 – 9) so that whether the platform is trusted or not can be determined accordingly (Grawrock: Column 4 Line 35 – 37 / Line 1 – 9 and Figure 3 / Element 340 & 345, 350 & 355 and 360 & 365). Besides, Examiner notes it absolutely makes no sense relying on an un-trusted party (i.e. a challenger) in verification (Grawrock: Column 4 Line 9) and determining that a computer entity is trustable (Grawrock: Column 4 Line 38).

Issue 2. **Claims 10, 27 and 45**: Whether claims 10, 27 and 45 are patentable under 35 U.S.C. 103(a) over Grawrock in view of U.S. Pat. No. 6,209,099 to Saunders (hereinafter "Saunders").

✓ Claim 10 depends from claim 7, claim 27 depends from claim 24, and claim 45 depends from claim 42. See the same rationale of rejections applying herein as set forth above in Issue 1 for base claims.

Issue 3. **Claims 20, 21, 38, 39, 41, 56, 57 and 59:** Whether claims 20, 21, 38, 39, 41, 56, 57 and 59 are patentable under 35 U.S.C. 103(a) over Grawrock in view of U.S. Pat. No. 6,615,264 to Stoltz (hereinafter "Stoltz").

✓ Claims 20 and 21 depend from claim 7, claims 38, 39 and 41 depend from claim 24, and claims 56, 57 and 59 depend from claim 42. See the same

rationale of rejections applying herein as set forth above in Issue 1 for base claims.

Issue 4. Claims 22 – 23 and 60 – 61: Whether claims 22-23 and 60-61 are patentable under 35 U.S.C. 103(a) over Grawrock.

✓ Claims 22-23 depend from claim 7, and claims 60-61 depend from claim 42. See the same rationale of rejections for base claims applying herein as set forth above in Issue 1.

Note: The appellant's statement of the status of EVIDENCE APPENDIX after final rejection contained in the brief is correct.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Longbit Chai

Conferees:

Kim Vu

Christopher A. Revak

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100